REMARKS

Prior to entry of this Amendment, Claims 14-21 and 50-65 were pending.

With this Amendment, Claims 14-18, 21, 50-55, and 58-62 have been amended. No Claims have been cancelled or added. No new matter is submitted. Claims 14-21 and 50-65 are now pending.

Rejections Under 35 U.S.C. §103(a)

1. Claims 14-21 and 50-65 stand rejected under 35 U.S.C. §103(a), as obvious in light of U.S. Publication No. 2002/0153424, to Li, in view of U.S. Publication No. 2002/0180584, to McGregor et al.

2. The Applicants respectfully traverse the rejections under 35 U.S.C. §103(a) as Claims 14-21 and 50-65 have been amended to obviate the obvious rejections of same. The Applicants respectfully request consideration of the following.

3. The present application, published as US PGPub No.: 2005/0053997, the "Publication"), discloses at paragraph [0029]:

> Each time the payment service is initiated, a dCVV is generated on the payment device for authentication purposes. FIG. 1 depicts the method of generating a dCVV for each transaction according to the present invention. Initially, a numeric string of predetermined length is created. This numeric string is created by overlaying 101 the ATC 102 over the corresponding leftmost digits of the account number for the payment service or PAN 104. This numeric string is concatenated on the right with the expiration date for the payment service and the service code to produce a concatenated value 106. If necessary, padding characters 108 are concatenated 110 on the right of the concatenated value 106 to form a numeric string 112 with a predetermined fixed length. In a preferred embodiment, this numeric string 112 is 128-bits in length, although a numeric string of any length may be used. The padding characters 108 may consist of a stream of 0's, 1's, or any other numeric value that is known both to the payment device and the service provider. The numeric string 112 is bisected into two blocks of equal length, Block A 116 and Block B 118. Block A 116 is then encrypted 121 with a first encryption key 120. The result of the encryption

> step 121 is Block C 122 of length equal to Block A 116. Block C 122 is then exclusively OR'ed (XOR) 123 with Block B 118 resulting in Block D 124. Block D 124 is then encrypted 125 with a second encryption key 126 to produce Block E 128. Block E 128 is then decrypted 129 using a decryption key 130 to produce Block F 132. Block F 132 is then encrypted 133 using a fourth encryption key 134 to produce Block G 136.

4. The pending claims have amended to recite elements found in the disclosure set forth at least in Figure 1 and paragraph 0029 of the present application. This disclosure teaches that a dynamic card verification value is generated on a payment device (e.g.; a smart card) for authentication purposes during a transaction on an account corresponding to the payment device. The dynamic card verification value is generated from a string of characters. The string of characters is created by overlaying an application transaction counter for the payment device over the leftmost digits of the primary account number for the account. The numeric string is concatenated on the right with the expiration date for the payment service and the service code to produce a concatenated value. If necessary, padding characters are concatenated on the right of the concatenated value to form a numeric string (which can be 128-bits in length). The numeric string is bisected into two blocks of equal length prior to performing encryption operations on each of the two blocks to form the generated dynamic card verification value.

5. The generated dynamic card verification value, advantageously, is sent to the point of sale terminal in the traditional format, namely in the magnetic stripe format which may be in the form of magnetic stripe credit card Track 1 and/or Track 2 data. As such, a contactless payment card is essentially treated as a traditional magnetic stripe payment card and transparent to the merchant's point of sale terminal by virtue of the continued use of the magnetic strips format for the transaction data.

6. The claimed invention recites a string of characters, ordered from left to right to include the primary account number, the application transaction counter, the expiration date, and the card service code. The dynamic card verification value is generated from the string of characters. As reflected in pending Claims 14-21 and 50-65, the mathematical manipulation of the uniquely composed and ordered string of characters to generate the recited verification value is not taught, suggested, or implied, either alone or in any combination, by the prior art of record.

7. US Patent No. 5,835,599 to Buer, also of record, teaches a well known Data Encryption Standard (DES) software technique that is accelerated by a novel hardware design. Buer, however, fails to teach encryption of the specifically ordered data string of account-centric data recited in the pending claims. The overlaid string of ordered account-centric data with the particular encryption thereof to create a verification value of a transaction, as recited, necessitate a finding that pending Claims 14-21 and 50-65 are neither anticipated by or obvious over any reference of record.

8. Given the foregoing, allowance of pending Claims 14-21 and 50-65 is respectfully requested.

CONCLUSION

Applicants hereby petition for any extension of time which may be required to maintain the pendency of this case, and any required fee, except for the Issue Fee, may be charged to **Deposit Account No. 17-0055**.

Should there by any additional issues which may be resolved by an interview, the Examiner is respectfully requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

QUARLES & BRADY LLP

Dated: October 27, 2009

By _____
Bradley K. DeSandro
Reg. No. 34,521

Address all correspondence to:

Bradley K. DeSandro
QUARLES & BRADY LLP
One Renaissance Square
Two North Central Avenue
Phoenix, AZ 85004
Telephone: (602) 229-5355
Facsimile: (602) 420-5022
E-mail: pat-dept@quarles.com